International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

Fast Flux &Fast Flux Detection Techniques : ASurvey

Jaya Jimiwal
Department of Computer Science and Engineering
Graphic Era Hill University
Dehradun

Abstract—**Botnet is the one of the largest security threats on the Internet. Botnet can be defined as a group of infected machines, called bots, is a predominate factor among all the internet malicious attacks such as DDoS, Spam and click fraud. Fluxing techniques are used to evade detection of botnet, employed by many owners of botnets such as Torpig, Conficker, worm, storm. A fast flux technique is a cycle of mapping of domain names to IP addresses of hosts participating in a botnet, has short lifetime mapping. In this paper we survey botnet, botnet life cycle and different techniques to detect fast flux, and there categories: Single Flux, Double Flux. we also define some techniques of domain fluxing. We focused on some research challenges to detect fast flux service network. We analyze the Fast Flux detection techniques by comparison using five criteria.**

Keywords— Botnet, Fast Flux (FF), Domain Flux (DF), Domain Name Server (DNS), Single Flux, Double Flux, Fast Flux Service Network (FFSN).

I. INTRODUCTION

A software program is used for unwanted action, called malicious software or malware. Now days the main idea behind writing malicious program is financial gain in current Internet based economic world. Malware allows malicious individuals to control computing devices remotely. The network of these computing devices is known as ***Botnet*** which use various forms of malware such as virus, worms, Trojan horse. In today's cybercrime activity, botnet is the launch pad on the Internet for evasion of these crimes.

Botnet is one of the largest security threats on the Internet. A botnet is a group of compromised computers, called bots or zombies, controlled by the botmaster's malware code. The botnets continuously improve the structure, protocols and attacks. The master computer uses a command and control(C & C) channel by which it communicates with its bots. C & C channel passes commands from the botmaster to bots and then it transmits stolen information from bots to their botmaster. Coordination among bots and their C & C servers is the main aspect of any botnet.

For implementing botnet command and control, the most popular methods are:

Internet Relay Chat (IRC) protocol based method: The main advantages of IRC based C&C channel are: 1. Ease of implementation. 2. Due to the simplicity of network, it forms large network very quickly. With many benefits, it also has a drawback that it has a centralized nature.

HTTP traffic based method: it hijacks a legitimate communication channel to bypass firewall based security. It is also facing the centralization problem.

Peer to peer network and protocol based method: It is more recent development in botnet C & C technology. In this method bot behaves as both client and server. So there is no issue of centralization. Day by day the botnets are very difficult to detect because of their advance mechanism. These mechanisms are:

1. Domain Flux (DF): A mechanism that have a unique IP address, corresponding to it domain name change frequently. In regular interval domain fluxing bots generates large numbers domain names to hide their tracks. Conficker, kraken, Srizbi and Torpig are some kind of botnet which use DNS domain fluxing to hide their C & C servers.

2. Fast flux (FF): A mechanism in which its having a unique domain name, corresponding to it IP address are change frequently. From many years fast flux techniques have been used by benign network for load balancing.

The network is called fast flux network (FFN), which apply fast flux technique. In the last few years, the use of FF techniques on malicious network has become popular. The benign and malicious network show almost same characteristics, such as TTL on DNS records. FFSN could be constructed as a distributed proxy network, with the help of the mapping techniques. Fast flux can be divided in two categories: Single Fast Flux and Double fast flux.

Single Fast Flux: In a single fast flux for a different time range, different IPs are used to mapping a particular domain.

Double Fast Flux: It provides additional redundancy. It involves the repeated changing of both the flux agents and the registrations in DNS server [3].

The survey paper is further explained as follows:

- Define the botnet &botnet life cycle, which is a popular tool used by hackers.
- Define fast flux and explained there work & techniques used by botnet to avoid the detection techniques.

- Finally compared the fast flux detection techniques using some criteria of their features.

In section second the background of the fast flux are explained, when fast flux firstly introduced by botnets, who firstly define the fast flux detection technique and what was the technique. Third section explains the fast flux and their detection techniques. Fourth section describes the comparison among fast flux detection techniques.

II. BACKGROUND

Honeynet [2] was the first project which describe about the fast flux mechanism of botnets. This paper describes all the malicious activities performed by botnets by using Single and double fast flux mechanism. Single fast flux mechanism use multiple IPs and it changes A records of domain rapidly while Double fast flux techniques change both A records and NS records frequently.

Holz et al. [1] present the first fast flux service network (FFSN) detection technique. They identified three parameters the no of IP- domain mappings in all DNS lookups , the no name server records in one single domain lookup and the no of autonomous system in all IP-domain pears. Based on these parameters they developed a matric that exploit the principal of FFSN. They also showed that method is accurate that means very low false positive and false negative rate. According to their observation they found other information, e.g., whois lookup and records.

Zhou et al. [4] introduced a behavior based analysis in his paper for the detection of fast flux in FFSNs. Detection is performed by characterizing the fast flux domain behavior. They showed the number of DNS queries, which conform FF domain with the help of an analytical model. They also present two schemas which are used to speed up the detection, one schema is to associate IP addresses with queries which results from multiple DNS servers and other schema is to co- relate queries, results with multiple FF domains. Through this technique we overcome from the limitations which focus on detecting domains.

Passerini et al. [5] developed FluXOR system which detect and monitors fast flux service networks. FluXOR monitor and detect based on the analysis of a set of features from the point of view of a victim. They define the three categories for the features: Domain name, availability of the network, Heterogeneity of the agents.

III. BOTNET AND FAST FLUX

This section provides the detail of Botnet and Fast Flux features of Botnet. The life cycle of Botnet are explained. Fast-Flux Botnet detection techniques are summarized.

A. Botnet Life Cycle

Botnet is maintained as a combination of infected machine. Feily et al. [6] describe the Botnet in five phases: Initial Infection, Secondary Injection, Connection, Malicious Command & Control, Update &Maintenance. In the other hand Zang et al. [7] explain Botnet life cycle in four phases.

Initial Phase: In the initial phase attacker infects the victim machine through different vulnerable methods, provide additional functionality to the attacker on a victim machine.

Secondary Injection: After initial phase, in secondary phase .The victim machine executes the malicious code after the installation of bot binary. The victim machine turns, became a bot and perform the malicious actions. To processed these procedure using FTP, HTTP, or TFTP.

In this figure:

1: Initial Infection, 2: Secondary Injection, 3: Connection & Update, 4: Maintenance & Update, 5: Maintenance & Update.

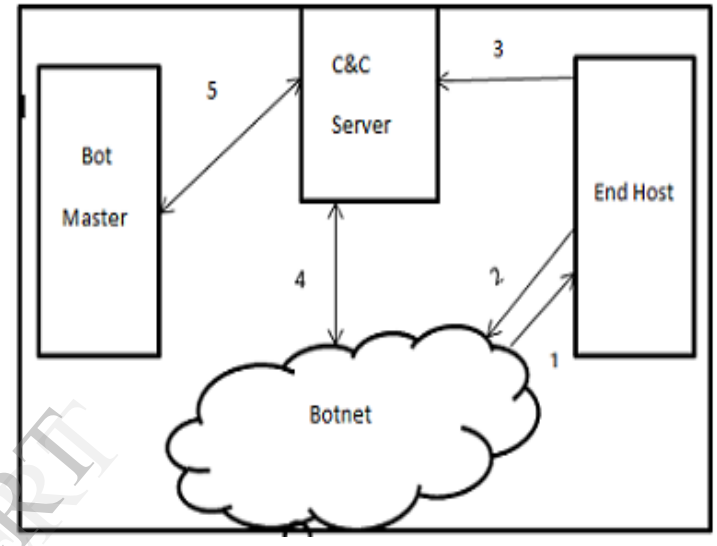

Figure 1: Botnet Life Cycle

Connection Phase: In connection phase the connection between C&C server and bot are establish using variety of methods, once the connection is establish the bot officially a part of attackers botnet.

Command & Control Phase: Once the connection ready the command &control activities are performing, most C&C protocol are designed by botnet specification.

Maintenance Phase: Last phase is to maintain & updated, the botmaster may need to update the bot to hide their unauthorized activity. Bot send an update command to C&C server to give the feedback of updated status.

B. Fast Flux

Fast-flux technique has been discovered in 2006 and since 2007 it's became a hot topic in botnet research. "Fast flux" is an evasion technique that used to evade identification by cyber-criminals and Internet miscreants. Botnet herders often use fast-flux DNS techniques to host unwanted or illegal content within a botnet. These techniques change the mapping of the domain name to different bots within the botnet with constant shifting, while the bots simply relay content back to a central server [16]. In the Botnet life cycle the Fast Flux is introduced after the completion of first two phases. Recent botnet are so difficult to be detects and perform delay in detection using fast flux to represent the ability to quickly move the location of a web, email, DNS or generally any Internet or distributed service from one or more computers

connected to the Internet to a different set of computers. We consider a domain name www.jay.com that using the fast flux mechanism. In the FFSN (Fast Flux Service Network) P, Q, R are fast flux agents for that domain. If a victim visits www.jay.com then queries a name server and directed by DNS to one of the agents (e.g. agent R). This agent than connect to the victim request to the mothership and give response back to the client. After some time if we again visit (www.jay.com) then DNS mapped the domain with different IP addresses so allow a different agent (e.g. agent P). Now we can see that the detection of Botmaster is difficult couse of Fast Flux.

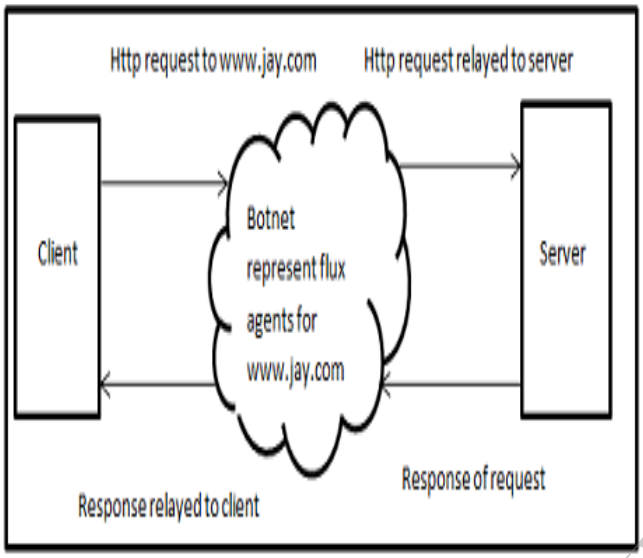

Figure 2: Fast Flux Network

Some botnet which are using Fast-Flux techniques are define here with their introducing date, features, functions, limitations and size.

Botnet	Year	Botnet Features	Function
Warezov [20, 21]	Sep-2006	Social Engineering, Rootkit	Email-attachment, harvest email addresses
Storm Botnet [5,19]	Jan-2007	Hash Encryption, Polymorphism	Spam, DDoS, Disable AVs
Waldac	Apr-2008	Hard coded Emails, URLs	Spam, Encryption Packer
Conficker	Mar-2009	DNS lookups, Transfer TCP, Scan-UDP	Self Defense machine,

Table 1: Fast-Flux based Botnets

C. Fast Flux Detection Techniques

Caglayan et al. [10] using 9 months collected database of FFSNs for fast flux service networks (FFSNs) behavioral analysis. Database of fast flux domain and IP collected by Fast Flux Monitor(FFM)which designed to detect whether a domain exhibits fast flux (FF) or double flux (DF) and real-time fast flux network detection algorithm. The result of this analysis show that such networks form clusters and share common characteristics of lifecycle. These characteristics are growth, size, and malicious behavior of different type.

2009 Perdisci et al. [9] propose an approach for detecting and tracking malicious flux service networks. They collected recursive DNS (RDNS) traffic traces from multiple large networks for passive analysis in detection system. In practice, front of the recursive DNS (RDNS) server of different networks deploy a sensor , the DNS queries and users to the RDNS responses are passively monitor, and potential fast-flux domains information selectively store into a central DNS data collector. Fast-flux domains are characterized by the following main features: a) short time-to-live (TTL); b) the set of resolved IPs (i.e., the flux agents) returned at each query changes rapidly, usually after every TTL; c) the overall set of resolved IPs obtained by querying the same domain name over time is often very large; d) the resolved IPs are scattered across many different networks [9]. Experimental results show that the proposed approach is able to accurately detect malicious flux service networks. Detection rate of domain names advertised through spam emails 90% to 95% accurate.

A.Caglayan et al. [8] using both active and passive DNS monitoring for detection of fast flux service networks in real time .Results show that Fast Flux Monitor can detect single and double flux behavior in real time. Three active sensors for FFM active sensors development , are: FF Activity Index, Footprint Index, and Time To Live (TTL), .They build a classifier using Bayesian belief network that fuses the multiple active and passive DNS sensors. This Bayesian classifier is trained to accept the TTL, Fast Flux Activity Index, and Footprint Index values. Results show that the collected fast flux database can be effectively queried to build automated reports for the security analyst.

Hsu et al. propose a way to detect a fast-flux botnet in real time which host a web service. The detection way is unique because of the characteristics of fast-flux bot-nets, in which the botnet relies. These are: i) the request delegation model, ii) bots are not dedicated to malicious services, and iii) the hardware used by bots is normally inferior to that of dedicated servers. Results show that, within a few seconds, detection of fast flux bots having more than 96% accuracy, while lower than 5% the false positive/negative rates. This schema using a passive measurement approach and achieves high accuracy but it has some limitations also, that are: i)A bot herder may compromise powerful servers and incorporate them into a fast-flux botnet. ii) A benign server may not be equipped with high-level hardware like the dedicated web servers provided by Internet service providers [11].

Stalmans et al. [12] examines geographic distribution of domain Servers based spatial autocorrelation techniques to detect Fast-Flux domains. They produce classifiers using multiple geographic co-ordinate systems to produce efficient

and accurate results. This paper show reliable process of detection Fast-Flux domains with a small percentage of false positives generation **Yu et al**. **[13]** analyzing the DNS queries pattern from fast flux botnets, and to detect these fast flux botnets using data mining technique. They develop a weighted SVM (support vector machine) for features extraction by which the fast flux and normal network domain are identified. They extract the six features and classified them into three categories: property of the domain, property of the network, and IP distribution of the flux agents. Results show that the weighted SVM is more efficient and accurate, generates low false positive in comparison to Holz linear classification algorithm.

Lin et al. [14] proposed a scheme for Fast-Flux Service Networks (FFSNs) detection known as Genetic-based Real-time Detection (GRADE).GRADE having six main components: IP extractor, ASN Query module, E-DPN measurement, SD-RRT measurement, weight –optimization module, and a FFSN detection engine. This schema provides high detection accuracy with low detection time. GRADE adds two new characteristics, to enhance the FFSNs detection accuracy. These characteristics are: Entropy of domains of preceding nodes for all A records (E-DPNs), Standard deviation of round trip times to all A records. If FFSN change continually than GRADE able to detect FFSN with high accuracy and low detection delay by applying genetic algorithm. Result show (~98%) accuracy within a few seconds.

Futai et al. [15] analyzing recursive DNS traffic and develop a detection method for fast-flux domain with the combination of both real-time detection and long term monitoring. In this paper J48 real time classifier achieves significantly lower false positive under each condition and two folds of detection as flux-score based algorithm does. Experimental results show that using this approach detection accuracy is higher in comparison to previous flux-score based algorithm.

IV. COMPERISION OF FAST FLUX TECHNIQUES

In this section, we compare the fast-flux (FF) detection techniques against multiple criteria. As we know, FF is very old techniques comparison to DF. A large amount of works has been done to detect FF botnets. Here, we use the following 5 criteria to analyze the fast flux detection techniques.

- Active & Passive
- Accuracy
- Algorithm
- Delay
- DNS based detection

Active & Passive: Perdisci et al. [9] using the passive approach for the detection of fast flux networks. Recursive Domain Name System traffic analyzed passively. Holz et al. [1] derived a metric "Flux Score" by which we detect fast flux domains through passive analysis. Hsu et al. [11], A.Caglayan et al. [10] using both the active and passive monitoring for fast flux networks detection.

Accuracy: Accuracy for fast flux detection is very important feature. If accuracy is high that means detection techniques are useful and security is high. A.Caglayan et al. [10] define a detection schema which provided 96% accuracy with less than 5% delay. Perdisci et al. [9] give high accuracy detection system using 12 features, according to these features the fast flux network or benign network are identified. If passively detect the system then the false positive rate is 0.7%. Holz et al. [1] developed a method for detection of fast flux with up to 99.98% accuracy. The False negative rate of the method is minimum which approximately 0.5% . Yu et al. [13] deigned a weighted support vector machine (SVM) using six features to define which domain is access by fast flux networks or which is access by normal networks. There detection accuracy is satisfactory.

Algorithm: Perdisci et al. [9] using hierarchical clustering algorithm by which the domain of same network are grouped together. Clustering algorithm detect the domains clusters of fast flux networks which is used by hackers or in phishing also. Yu et al. [13] define the linearly based separable problem. To solve this kind of problem design a SVM algorithm based on linear kernel function. SVM algorithm performs better in terms of false positive rate comparison to other linear algorithm.

Delay: Delay is inversely proportional to accuracy. If delay is low then accuracy is high and vice versa. Hsu et al. [11] having detection technique with low delay time, (<5%) less than 5% with a very high accuracy.

DNS based detection: Most of the detection techniques based on their DNS traffic analysis. The detection techniques explained in this paper are DNS based. Perdisci et al. [9] detecting the fast flux by analyzing the recursive DNS traffic. Yu et al. [13] trace the DNS records using data mining techniques. A.Caglayan et al. [10] and Hsu et al. [11] apply both the active and passive approach for fast flux networks detection in which the A.Caglayan detection based on Domain Name system upcoming and outgoing records.

Detection Techniques	Active/ Passive	Algo.	Accuracy	Delay	DNS Based Detection
Recursive DNS [9]	P	Hierarchical Clustering	High	Low	Yes
FF Botnet [11]	A &P	Decision	High	Low (<5)	-
Flux Score [1]	P	Linear Classifier	High	-	Yes
FF Monitor [10]	A &P	-	Acceptable	-	Yes
SVM[13]	-	SVM Algorithm	Sufficient	Low	Yes

Table 2: Comparisons of Fast-Flux Detection Techniques

IV. CONCLUSION

This paper explain the botnet, there life cycle, fast flux and fast flux detection techniques. Readers can gain detail understanding of fast flux and there detection techniques. Paper define the fast flux model by which we can easily understand how fast flux work and how it's using there FF (Fast Flux) and DF (Domain Flux) features for evasion of detection. Comparing the fast flux detection techniques using some criteria of theirs features. By which reader can easily understand the better detection techniques among them and which one is more accurate.

ACKNOWLEDGEMENT

I would like to thank my teachers for their guidance , my Parents and friends for their help , viewers for their comments through which I am able to write this survey paper.

REFERENCES

[1] Holz, T.Gorecki, C.Rieck, C.Freiling, F. "Measuring and Detecting Fast-Flux Service Networks." Presented at NDSS Symposium (2008).

[2] Honeynet, "How fast flux service network work." http://www.honeynet.org/node/132,2008.

[3] Lei Zhang, Shui Yu, Diwu, Paul Watters, "A survey on latest Botnet Attack & Defense." In International joint conference, 2011.IEEE ICESS-11.

[4] C.V.Zhow, C.Lickie, and S.Karunas ekera, "Collaborative Detection of Fast Flux Phishing Domains." JNW, vol. 4, no, PP.75-84, 2009.

[5] Emanuele Passerini, Roberto Paleari, Lorenzo Martiganoni, and D.Bruschi, "FluXOR: Detecting and Monitoring Fast Flux Service Networks, 2008.

[6] Maryam Feily, Alireza Shahrestani, "A survey of Botnet and Botnet Detection." Third International Conference on Emerging Security Information, Systems and Technologies, 2009.

[7] Xiaonon Zang, Athichart Tangpong, George Kesidis and David J.Mikker, "Botnet Detection Through Fine Flow Classification." CSE Dep. Technical Report No.CSE 11-001, jan.31, 2011.

[8] Alper Caglayan, Mike Toothaker, Dan Draoaeau, Dussin Burke, Gerry Eaton, " Behavioral Analysis of Fast Flux Service Networks.", 5th Annual Workshop on Cyber Security & Information Intelligence Research: Cyber Security Intelligence Challenges & Strategies2009.

[9] Roberto Perdisci, Igino Corona, David Dagon, and Wenke Lee, "Detecting Malicious Flux Service Networks through Passive Analysis of Recursive DNS Traces." In: Annul Computer Socitey Security Applications Conference (ACSAC), 2009.

[10] Alper Caglayan, Mike Toothaker, Dan Drapeau, Dustin Bruke, Gerry Eaton, "Real Time Detection of Fast Flux Service Networks.", In Cyber Security Applications & Technology Conference for Homeland Security, IEEE 2009.

[11] Ching-Hsiang Hsu, Chun-Ying Huang, Kuan-Tachen, "Fast-Flux Bot Detection in Real time." Recent Advance in Intrusion Detection, Pages 464-483, 2010.

[12] E.Stalmans, S.O.Hunter, B.Irwin, "Geo-spatial Autocorrelation as a Metric for the Detection of Fast-Flux Botnet Domains.", In: Information Security for South Africa (ISSA), 2012. P. 1-7.

[13] Xiangzhan Yu, BoZhang, LeKang, Juan Chen, "Fast-Flux Botnet Detection Based on Weighted SVM." In: Proceedings of Information Technology Journal; 2012. P. 1048-1055.

[14] Hui-Tang Lin, Ying-You Lin, Jui-Wei Chiang "Genetic-based Real-time Fast Flux Service Networks Detection.", In computer networks 2013, P.501-513.

[15] Zou Futai, Zhang Siyu, Rao Weixiong, "Hybrid Detection and Tracking of Fast-Flux Botnet on Domain Name System Traffic.", 2013.P.81-94.

[16] Jose Nazario, Thorsten Holz: "As the Net Churns: Fast- Flux Botnet Observations." In: Inter-national Conference on Malicious and Unwanted Software, MALWARE (2008).

[17] S.Yu, S.Zhou, and S.Wang, "Fast-Flux attack network identification based on agent lifespan." In Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on, June 2010, PP.658-662.

[18] Basheer N.Al- Duwairi, Ahmad T. Al- Hammouri, "Fast Flux Watch: A mechanism for online detection of fast flux networks", in: Journal of Advanced Research, 2014.

[19] Phillip Porras and Hassen Saidi and Vinod Yegneswaran, "A Multi-Perspective Analysis of the Storm (Peacomm) Worm.", CSL technical note, SRI International, 2007.

[20] Wikipedia: en.wikipedia.org/wiki/stration.

[21] F-secure: http://www.f-secure.com/v-descs/warezov.shtml.